CLAIMS

What is claimed is:

1. A method for controlling access to a resource, the method comprising the steps of:

creating and storing in the Operating System filesystem a file that represents the resource;

receiving user-identifying information from a user requesting access to the resource, wherein the user-identifying information comprises a role associated with the user, wherein the role is determined from a user identifier uniquely associated with the user and from a group identifier associated with a group that includes the user;

receiving a resource identifier associated with the resource;

creating an access identifier based on the user-identifying information and the resource identifier, wherein the access identifier is formatted as a file attribute that is used by the Operating System to manage file access;

calling the Operating System to perform an operation on the file using the access identifier to gain access to the file; and

granting the user access to the resource only if the Operating System call successfully performs the operation.

2. A method as recited in Claim 1, wherein the access identifier comprises:

a first set of bits for storing a role identifier, wherein the role identifier is associated with the role; and

a second set of bits for storing the resource identifier.

3. A method as recited in Claim 1, wherein:

the step of creating an access identifier based on the user-identifying information and the resource identifier comprises formatting the access identifier as a group identifier file attribute; and

the step of calling the Operating System to perform an operation on the file representing the resource comprises:

assigning the access identifier to a group identifier attribute of an Operating System process; and calling an Operating System routine from the Operating System process to perform the operation on the file representing the resource.

4. A method as recited in Claim 1, wherein the step of calling the Operating System to perform an operation on the file representing the resource comprises comparing the access identifier to an identifier included in an Access Control List file attribute associated with the file representing the resource, wherein the Access Control List file attribute includes the identifiers of all users and all groups of users allowed to access the file representing the resource.

5. A method as recited in Claim 1, wherein the operation on the file representing the resource is selected from a group consisting of opening the file, closing the file, deleting the file, reading from the file, writing to the file, executing the file, appending to the file, reading a file attribute, and writing a file attribute.

6. A method as recited in Claim 1, the method further comprising the steps of:

reading a permission bit associated with the file representing the resource, wherein the permission bit corresponds to a file operation performable on the file representing the resource;

based on the file operation indicated by the permission bit, determining a resource operation that is performable on the resource; and

granting the user the privilege of performing the resource operation on the resource only if the permission bit allows the file operation to be performed on the file representing the resource.

7. A method as recited in Claim 1, the method further comprising the steps of:

opening the file representing the resource;

reading from the file representing the resource a permission indicator associated with a resource operation; and

enabling the user to perform the resource operation on the resource only if the permission indicator indicates that the user is allowed to perform the resource operation on the resource.

8. A method as recited in Claim 1, wherein the step of representing the resource by a file stored in the Operating System filesystem comprises:

creating the file representing the resource in the Operating System filesystem; and

assigning an access value to a file attribute of the file representing the resource, the file attribute being used by the Operating System to manage file access, wherein the access value corresponds to a combination of a role and a resource.

9. A method as recited in Claim 8, wherein the file attribute used by the Operating System to manage file access is a group identifier file attribute.

10. A method for controlling access to a resource, the method comprising the steps of:

receiving a user identifier from a user requesting access to the resource, wherein the user identifier is uniquely associated with the user;

receiving a group identifier associated with a group to which the user belongs;

based on the user identifier and the group identifier, determining a role associated with the user, wherein a role identifier is uniquely associated with the role;

receiving a resource identifier associated with the resource, wherein the resource is represented by a file stored in the Operating System filesystem;

constructing an access identifier on the basis of the role identifier and the resource identifier, wherein the access identifier conforms to the format of a group identifier file attribute that is used by the Operating System to manage file access;

making an Operating System call to perform an operation on the file representing the resource, wherein the Operating System call uses the access identifier to gain access to the file representing the resource; and

granting the user access to the resource only if the Operating System call successfully performs the operation on the file representing the resource.

11. A method as recited in Claim 10, wherein the access identifier comprises:

a first set of bits for storing the role identifier, wherein the role identifier represents a bitmap, each bit of the bitmap uniquely associated with a role of the user; and

a second set of bits for storing the resource identifier.

12. A method as recited in Claim 10, wherein the step of making an Operating System call to perform an operation on the file representing the resource comprises:

storing the group identifier value of a group identifier attribute of an Operating System process;

assigning the access identifier to the group identifier attribute of the Operating System process;

calling an Operating System routine from the Operating System process to perform the operation on the file representing the resource, wherein the operation on the file representing the resource is performed only if the value of the group identifier attribute of the Operating System process matches the value of the group identifier file attribute of the file representing the resource; and

resetting the group identifier attribute of the Operating System process to the stored group identifier value.

13. A method as recited in Claim 10, wherein the step of making an Operating System call to perform an operation on the file representing the resource comprises comparing the access identifier to an identifier included in an Access Control List file attribute associated with the file representing the resource, wherein the Access Control List file attribute includes the identifiers of all users and all groups of users allowed to access the file representing the resource.

14. A method as recited in Claim 10, wherein the operation on the file representing the resource is selected from a group consisting of opening the file, closing the file, deleting the file, reading from the file, writing to the file, executing the file, appending to the file, reading a file attribute, and writing a file attribute.

15. A method as recited in Claim 10, the method further comprising the steps of:

reading a permission bit associated with the file representing the resource, wherein the permission bit corresponds to a file operation performable on the file representing the resource;

based on the file operation indicated by the permission bit, determining a resource operation that is performable on the resource; and granting the user the privilege of performing the resource operation on the resource only if the permission bit allows the file operation to be performed on the file representing the resource.

16. A method as recited in Claim 10, the method further comprising the steps of:

opening the file representing the resource;

reading from the file representing the resource a permission indicator associated with a resource operation; and

granting the user the privilege of performing the resource operation on the resource only if the permission indicator indicates that the user is allowed to perform the resource operation on the resource.

17. A method as recited in Claim 10, the method further comprising:

creating the file representing the resource in the Operating System filesystem; and

assigning an access value to a group identifier file attribute of the file representing the resource, the group identifier file attribute being used by the Operating System to manage file access, wherein the access value is uniquely determined by the combination of a role and a resource.

18. A system for controlling access to a resource connected to a network, the system comprising:

a client host capable of accessing the resource in response to a request for access from a user;

one or more processors executing an Operating System, wherein the Operating System operatively controls a filesystem that includes a number of files; and

a computer readable medium having stored therein an Application Programming Interface, wherein the Application Programming Interface is logically interposed between the client host and the Operating System and comprises one or more routines including routines which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

creating and storing in the filesystem a file that represents the resource;

receiving user-identifying information from the user requesting access to the resource, wherein the user-identifying information comprises a role associated with the user, wherein the role is determined from a user identifier uniquely associated with the user and from a group identifier associated with a group that includes the user;

receiving a resource identifier associated with the resource;

creating an access identifier based on the user-identifying information and the resource identifier, wherein the access identifier is formatted as a file attribute that is used by the Operating System to manage file access;

calling the Operating System to perform an operation on the file using the access identifier to gain access to the file; and

granting the user access to the resource only if the Operating System call successfully performs the operation.

19. A system as recited in Claim 18, wherein the access identifier comprises:

a first set of bits for storing a role identifier, wherein the role identifier is associated with the role; and

a second set of bits for storing the resource identifier.

20. A system as recited in Claim 18, wherein:

the step of creating an access identifier based on the user-identifying information and the resource identifier comprises formatting the access identifier as a group identifier file attribute; and

the step of calling the Operating System to perform an operation on the file representing the resource comprises:

assigning the access identifier to a group identifier attribute of an Operating System process; and

calling an Operating System routine from the Operating System process to perform the operation on the file representing the resource.

21. A system as recited in Claim 18, wherein the operation on the file representing the resource is selected from a group consisting of opening the file, closing the file, deleting the file, reading from the file, writing to the file, executing the file, appending to the file, reading a file attribute, and writing a file attribute.

22. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 1.

23. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 2.

24. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 3.

25. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 4.

26. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 5.

27. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 6.

28. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 7.

29. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 8.

30. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 9.

31. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 10.

32. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 11.

33. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 12.

34. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 13.

35. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 14.

36. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 15.

37. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 16.

38. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the method recited in Claim 17.